

Measurement-based quantum computation cannot avoid byproducts

Tomoyuki Morimae*

*Controlled Quantum Dynamics Theory Group,
Imperial College London, London SW7 2AZ, United Kingdom*

(Dated: August 29, 2012)

*Electronic address: morimae@gmail.com

Measurement-based quantum computation [1] is a novel model of quantum computing where universal quantum computation can be done with only local measurements on each particle of a quantum many-body state, which is called a resource state [1–13]. One large difference of the measurement-based model from the circuit model is the existence of “byproducts”. In the circuit model, a desired unitary U can be implemented deterministically, whereas the measurement-based model implements BU , where B is an additional operator, which is called a byproduct. In order to compensate byproducts, following measurement angles must be adjusted. Such a feed-forwarding requires some classical processing and tuning of the measurement device, which cause the delay of computation and the additional decoherence. Is there any “byproduct-free” resource state? Here we show that if we respect the no-signaling principle [14], which is one of the most fundamental principles of physics, no universal resource state can avoid byproducts.

I. NO-SIGNALING PRINCIPLE

The no-signaling principle means that no message can be transmitted immediately. It is one of the most central principles in physics, and it is known to be more fundamental than quantum physics in the sense that there is a no-signaling theory which is more non-local than quantum physics [14].

The definition of the no-signaling principle is as follows [14]. Let us assume that Alice and Bob share a physical system, which might be classical, quantum, or even super-quantum system (Fig. 1). Each of them measure their own part. Then, the no-signaling means

$$\sum_a P(a, b|x, y) = \sum_a P(a, b|x', y)$$

for all b , x , x' , and y . Here, a is Alice’s measurement result, b is Bob’s measurement result, x represents Alice’s measurement choice, and y represents Bob’s measurement choice. Intuitively, this equation means that even if Alice changes her measurement choice, Bob’s measurement result is not affected.

II. MEASUREMENT-BASED QUANTUM COMPUTATION

We perform measurement-based quantum computation on the quantum many-body system S whose state is ρ . In other words, ρ is the resource state of our measurement-based

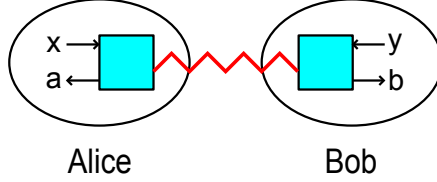


FIG. 1: **The setup for the no-signaling principle.** Alice and Bob share a physical system. Alice inputs x and obtains the output a . Bob inputs y and obtains the output b .

quantum computation. We divide S into two subsystems M and O such that $S = M \cup O$ and $M \cap O = \phi$. The subsystem M is the set of particles to be measured, and the subsystem O is the set of particles which contains the quantum output at the end of the computation (Fig. 2).

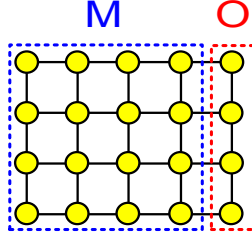


FIG. 2: **The resource state.** The set M of particles to be measured, and the set O of particles which contains the quantum output state at the end of the computation.

Let us assume that our quantum computation is the implementation of a unitary operator U on the initial state σ . For that purpose, we measure all particles in M . After the measurement, the state of the subsystem O becomes

$$B_k U \sigma U^\dagger B_k^\dagger$$

with probability p_k , where k is a vector which represents specific measurement results (a branch), and B_k is the byproduct corresponding to k . If $B_k = I$ for all k , this means that the resource state ρ is “byproduct free” for U .

For example, let us consider the one-dimensional cluster state [1]. If we measure a qubit of the cluster state, we can implement $X^s H e^{iZ\theta/2}$ if the measurement result is $s = 0, 1$, respectively. These two measurement outcomes occur with the equal probability. Therefore, in the cluster model, $X^p Z^q U$, where $p, q \in \{0, 1\}$, is implemented with equal probabilities

1/4. Although such a byproduct $X^p Z^q$ plays a crucial role in some secure computation, such as blind quantum computation [15–23], it would be desirable for a scalable quantum computation if we could find a resource state which is byproduct free, since byproducts require feed-forwarding, and it causes an additional decoherence. However, we show that due to the no-signaling principle, no universal resource state is byproduct free.

III. PROOF

In order to show it, let us consider measurement-based quantum computation between two people, Alice and Bob, as is shown in Fig. 3. Alice and Bob first share the resource state ρ (Fig. 3 (a)). Alice possesses the subsystem M and Bob possesses the subsystem O . Next Alice measures each particle of M (Fig. 3 (b)). After Alice measuring all particles of M , the subsystem O , which Bob has, is in the state

$$B_k U \sigma U^\dagger B_k^\dagger$$

with the probability p_k from Alice's view point (Fig. 3 (c)). From Bob's view point, the state of the subsystem O is

$$\sum_k p_k B_k U \sigma U^\dagger B_k^\dagger,$$

since Bob does not know k . Let us assume $B_k = I$ for all k . Then, Bob's state is

$$\begin{aligned} \sum_k p_k B_k U \sigma U^\dagger B_k^\dagger &= \sum_k p_k U \sigma U^\dagger \\ &= U \sigma U^\dagger. \end{aligned}$$

Let us choose a unitary operator V such that

$$V \sigma V^\dagger \neq U \sigma U^\dagger.$$

Because ρ is a universal resource state, the implementation of V is also possible with appropriate measurements on M . Then, if we repeat the above argument by replacing U with V , what Bob finally obtains after the two-party measurement-based quantum computation (Fig. 3 (c)) is

$$V \sigma V^\dagger$$

if ρ is byproduct free for V . However, since we have assumed

$$V\sigma V^\dagger \neq U\sigma U^\dagger,$$

it contradicts to the no-signaling principle. In other words, if there exists a byproduct-free universal resource state, Alice can have Bob possess two different states, $U\sigma U^\dagger$ or $V\sigma V^\dagger$, at her will by choosing her measurement pattern on M . It contradicts to the no-signaling principle, since she can exploit it to transmit her message to Bob.

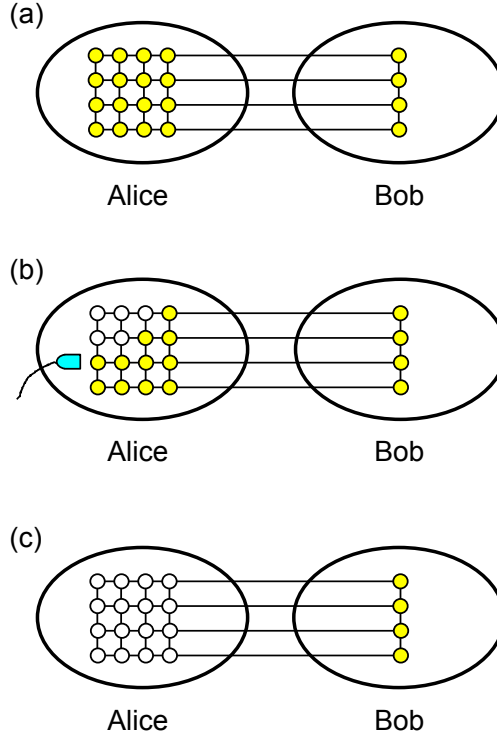


FIG. 3: **Measurement-based quantum computation between Alice and Bob.** (a) Alice and Bob share the resource state. (b) Alice measures each particle according to her algorithm. (c) Bob has the output state.

IV. DISCUSSION

In this paper, we have shown that if we respect the no-signaling principle, no universal resource state of measurement-based quantum computation can be byproduct free.

In the above argument, we have considered the deterministic measurement-based quantum computation. In other words, we have assumed that a desired unitary operator can be

implemented up to byproducts by measuring a *fixed* number of particles. For example, the cluster state allows such a deterministic measurement-based quantum computation. However, there are some resource states which allow only non-deterministic measurement-based quantum computation. For example, let us consider the one-dimensional Affleck-Kennedy-Lieb-Tasaki (AKLT) state [2, 24], which is a chain of spin-1 (qutrit) particles. If we measure a qutrit, we can implement $Xe^{iZ\theta/2}$, $XZe^{iZ\theta/2}$, or Z according to the measurement result. Note that if we obtain the third measurement result, we cannot implement the z -rotation, and we just obtain the trivial Z operation. Hence a desired unitary operator can be implemented up to byproducts with the probability $1 - 3^{-r}$ if we measure r qutrits.

In this case, a similar argument leads to

$$(1 - 3^{-r})U\sigma U^\dagger + 3^{-r}F_U\sigma F_U^\dagger = (1 - 3^{-r})V\sigma V^\dagger + 3^{-r}F_V\sigma F_V^\dagger,$$

where F_U and F_V are some “failed” operators, which are bounded. Then, we obtain

$$\begin{aligned} \|U\sigma U^\dagger - V\sigma V^\dagger\| &= \frac{3^{-r}}{1 - 3^{-r}} \|F_V\sigma F_V^\dagger - F_U\sigma F_U^\dagger\| \\ &\leq \frac{3^{-r}}{1 - 3^{-r}} (\|F_V\sigma F_V^\dagger\| + \|F_U\sigma F_U^\dagger\|), \end{aligned}$$

which again leads to the contradiction if we choose V in such a way that it is sufficiently different from U .

Acknowledgments

The author acknowledges JSPS for support.

-
- [1] Raussendorf, R. & Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett.* **86**, 5188 (2001).
 - [2] Brennen, G & Miyake, A. Measurement-based quantum computer in the gapped ground state of a two-body Hamiltonian. *Phys. Rev. Lett.* **101**, 010502 (2008).
 - [3] Miyake, A. Quantum computation on the edge of a symmetry-protected topological order. *Phys. Rev. Lett.* **105**, 040501 (2010).
 - [4] Miyake, A. Quantum computational capability of a 2D valence bond solid phase. *Ann. Phys.* **326**, 1656-1671 (2011).

- [5] Wei, T. C., Affleck, I. & Raussendorf, R. Affleck-Kennedy-Lieb-Tasaki state on a honeycomb lattice is a universal quantum computational resource. *Phys. Rev. Lett.* **106**, 070501 (2011).
- [6] Gross, D. & Eisert, J. Novel schemes for measurement-based quantum computation. *Phys. Rev. Lett.* **98**, 220503 (2007).
- [7] Morimae, T. Quantum computational tensor network on string-net condensate. *Phys. Rev. A* **85**, 062328 (2012).
- [8] Chen, X., Zeng, B., Gu, Z., Yoshida, B. & Chuang, I. L. Gapped two-body Hamiltonian whose unique ground state is universal for one-way quantum computation. *Phys. Rev. Lett.* **102**, 220501 (2009).
- [9] Fujii, K. & Morimae, T. Topologically protected measurement-based quantum computation on the thermal state of a nearest-neighbor two-body Hamiltonian with spin-3/2 particles. *Phys. Rev. A* **85**, 010304(R) (2012).
- [10] Li, Y., Browne, D. E., Kwek, L. C., Raussendorf, R. & Wei, T. C. Thermal states as universal resources for quantum computation with always-on interactions. *Phys. Rev. Lett.* **107**, 060501 (2011).
- [11] Cai, J., Miyake, A., Dür, W. & Briegel, H. J. Universal quantum computer from a quantum magnet. *Phys. Rev. A* **82**, 052309 (2010).
- [12] Menicucci, N. C., van Loock, P., Gu, M., Weedbrook, C., Ralph, T. C. & Nielsen, M. A. Universal quantum computation with continuous-variable cluster states. *Phys. Rev. Lett.* **97**, 110501 (2006).
- [13] Morimae, T. & Fujii, K. Not all physical errors can be linear CPTP maps in a correlation space. *Scientific Reports*, **2**, 508 (2012).
- [14] Popescu, S. & Rohrlich, D. Quantum nonlocality as an axiom. *Found. Phys.* **24**, 379-385 (1994).
- [15] Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. *Proc. of the 50th Annual IEEE Sympo. on Found. of Comput. Sci.* 517-526 (2009).
- [16] Fitzsimons, J. & Kashefi, E. Unconditionally verifiable blind computation. Preprint at arXiv:1203.5217 (2012).
- [17] Barz, S., Kashefi, E., Broadbent, A., Fitzsimons, J., Zeilinger, A. & Walther, P. Demonstration of blind quantum computing. *Science* **335**, 303-308 (2012).
- [18] Dunjko, V., Kashefi, E. & Leverrier, A. Blind quantum computing with weak coherent pulses. *Phys. Rev. Lett.* **108**, 200502 (2012).

- [19] Morimae, T., Dunjko, V. & Kashefi, E. Ground state blind quantum computation on AKLT state. Preprint at arXiv:1009.3486 (2010).
- [20] Morimae, T. & Fujii, K. Blind topological measurement-based quantum computation. Preprint at arXiv:1110.5460 (2011); to be published in Nature Communications.
- [21] Morimae, T. Continuous-variable blind quantum computation. Preprint at arXiv:1208.0442 (2012).
- [22] Morimae, T. No-signaling topological quantum computation in intelligent environment. Preprint at arXiv:1208.1495 (2012).
- [23] Morimae, T. & Fujii, K. Blind quantum computation for Alice who does only measurements. Preprint at arXiv:1201.3966 (2012).
- [24] Affleck, I., Kennedy, T., Lieb, E. H. & Tasaki, H. Valence bond ground states in isotropic quantum antiferromagnets. *Comm. Math. Phys.* **115**, 477-528 (1988).